UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/773,793 | 02/05/2004 | Koo-Hong Kang | 3364P162 | 8460 |

8791 7590 11/08/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

| EXAMINER | |
|---|---|
| MAUNG, ZARNI | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2151 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/08/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/773,793 | KANG ET AL. | |
| | Examiner | Art Unit | |
| | Zarni Maung | 2151 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *05 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/6/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1. This action is responsive to the application filed on February 5, 2004. Claims 1-12 are presented for examination.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gordy et al., U.S. Patent Number 6,898,632 (hereinafter Gordy), in view of Lee et al., U.S. Patent Application Publication US 2004/0093520 A1 (hereinafter Lee).

Gordy discloses a method and a system for detecting intrusion of computer networks. Gordy discloses the invention substantially as claimed. Taking claim 1 as an

exemplary claim, Gordy discloses, in a system coupled between a protection network (111) and an external network (115), for detecting intrusion states between the protection and external networks and preventing the intrusion, wherein an in-line mode network intrusion detecting and preventing system (100A) comprising: a first network processor unit for monitoring an externally received PDU (packet data unit), collecting various statistical data according to a metering rule, selectively discarding or passing the received PDU according to a packet preventing rule, and generating a duplicate of the PDU according to a sensing rule (see figures 3-6, firewall 108, routing node, Ethernet switch 302, processor 336, col. 3, lines 1-31); a second network processor unit for applying at least one attack signature to a payload of the PDU received from the first network processor unit and detecting intrusion states between the protection and external networks (see figure 2A, col. 7, line 57 to col. 8, line 30, Intrusion detection system 116 compares the signals to attack signatures), and hardware component system (Tab 300) for generating or updating a packet preventing rule for preventing the intrusion detected by the second network processor unit, and providing the packet preventing rule to the first network processor unit (see figures 2A, 3-7, col. 7, line 58 to col. 8, line 57, col. 10, line 20 to col. 11, line 52; Embodiments of circuitry and components of security taps section).

Gordy does not explicitly show a personal computer as recited in the claim; however, Gordy discloses hardware Tab components for performing equivalent functions of the claimed personal computer. Lee, in the same field of endeavor, discloses a system for detecting intrusion of computer networks; wherein Lee discloses

an improvement to a system similar in configuration to that of Gordy using a personal instead of hardware tab components (see figure 3, elements 210, 260 and the general-purpose computer 220). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to recognize that the functions of hardware Tab in the system disclosed by Gordy can be replace with a personal computer as shown in the improvement disclosed by Lee (see [0037], [0044]). One skilled in the art would have been motivated to modify Gordy in view of Lee to include a personal computer so as to enabled an intrusion system with a variety of functions as suggested by Lee (see [0044]).

4. As per claim 2, Gordy discloses the system of claim 1, further comprising a line interface for transmitting at least one PDU received from an external Ethernet interface to the first network processor unit (see Ethernet switch 302, and associated connections).

5. As per claim 3, Gordy discloses the system of claim 2, wherein the hardware tabs generates or updates a packet preventing rule and a sensing rule which include at least one of a transmitter port address and a destination port address of the PDU, a transmitter IP (Internet protocol) address, a destination IP address, a protocol, and a TCP (transmission control protocol) flag bit or which include a combination of at least two of them (see col. 7, line 53 to col. 8, line 30, operation of the test equipment and intrusion detection system IDS). Gordy does not explicitly show a personal computer

as recited in the claims. However, it would have been an obvious modification for one of ordinary skill in the art at the time the invention was made to use a personal computer instead of hardware Tab in the system disclosed by Gordy in view of the improvement disclosed by Lee for the same reasons set forth in claim 1.

6. As per claim 4, Gordy discloses the system of claim 3, wherein the hardware Tab generates or updates a metering rule which includes at least one of a transmitter Ethernet address, a destination Ethernet address, and an Ethernet type of the PDU, a transmitter IP address, a destination IP address, a transmitter port address, a destination port address, a protocol, and a TCP flag bit or which includes combinations of at least two of them (see col. 7, line 53 to col. 8, line 30, operation of the test equipment and intrusion detection system IDS). Gordy does not explicitly show a personal computer as recited in the claims. However, it would have been an obvious modification for one of ordinary skill in the art at the time the invention was made to use a personal computer in view of the improvement disclosed by Lee for the same reasons set forth in claim 1.

7. As per claim 5, Gordy discloses the system of claim 4, wherein the first network processor unit comprises: a sorter for determining whether to discard or pass the PDU received from the line interface according to the packet preventing rule received from the personal computer, and determining whether to duplicate the received PDU according to the sensing rule received from the personal computer; a traffic manager for

discarding the received PDU or duplicating the PDU determined to be sensed thereby generating a duplicate of the PDU, according to a discarding determination by the sorter; and a state engine for managing various statistical data relating to the PDU received from the line interface, according to the traffic metering rule received from the personal hardware tab (see col. 7, line 10 to col. 8, line 30, operation of the test equipment, intrusion detection system IDS, and Tab component). Gordy does not explicitly show a personal computer as recited in the claims. However, it would have been an obvious modification for one of ordinary skill in the art at the time the invention was made to use a personal computer in view of the improvement disclosed by Lee for the same reasons set forth in claim 1.

8. As per claim 6, Gordy discloses the system of claim 5, wherein the first network processor unit further comprises: first to fourth logic ports for outputting the PDU to the Ethernet interface, or receiving the PDU from the Ethernet interface; a link layer receiver for receiving the duplicate of the PDU from the state engine; a PDU converter/duplicator for generating a BPDU (bearer PDU) and an SPDU (shortened PDU) by using the received duplicate of the PDU; and a PHY transmitter for transmitting the generated BPDU and the SPDU to the second network processor unit (see figures 2-7, operations of the routing node, test equipment and IDS).

9. As per claim 7. The system of claim 6, wherein the second network processor unit comprises: a sorter for performing pattern matching on the payloads of the

transmitted BPDU and the SPDU according to the rule received from the personal computer, and detecting the intrusion state between the protection and external networks; a state engine for collecting and managing information on the detected intrusion state; and a PCI interface for transmitting the collected and managed information to the personal computer (see figures 2-7, operations of the routing node, test equipment and IDS).

10. As per method claims 8-12, they are directed to method for operating the system as set forth in claims 1-7; and they do not teach or further define over the limitations recited in claims 1-7. Therefore, claims 8-12 are also rejected for the similar reasons set forth claims 1-7, *supra*.

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see attached PTO-982).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zarni Maung whose telephone number is (571) 272-3939. The Examiner can normally be reached on Monday-Friday from 8:30 to 5:00 p.m. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's Supervisor, John Follansbee can be reached at (571) 272-3964. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3800/4700.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system, status information for published application may be obtained from either Private or Public PAIR, for unpublished application Private PAIR only (see http://pair-direct.uspto.gov or the Electronic Business Center at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

**Commissioner of Patents and Trademarks**
**P.O. Box 1450**
**Alexandria, VA 22313-1450**

Hand carried or delivered to:
Customer Service Window located at the Randolph Bldg. 401 Dulany St. Alexandria, VA 22314
Faxed to the Central Fax Office:
(571) 273-8300 (New Central Fax No.)
Or Telephone
(571) 272-2100 for TC 2100 Customer Service Office.

ZARNI MAUNG
PRIMARY EXAMINER